JEKEM
An ICA Institute Publication

INDIA, CHINA AND AMERICA INSTITUTE
1549 CLAIRMONT ROAD, SUITE 202 ● DECATUR, GA 30033 USA
WWW.ICAINSTITUTE.ORG

An Exploration of Human Resource Management Information Systems Security

Humayun Zafar, Jan G. Clark & Myung S. Ko

Journal of Emerging Knowledge on Emerging Markets
Volume 3
November 2011

An Exploration of Human Resource Management Information Systems Security

Humayun Zafar
Kennesaw State University

Jan G. Clark
The University of Texas at San Antonio

Myung S. Ko
The University of Texas at San Antonio

Journal of Emerging Knowledge on Emerging Markets
Volume 3
November 2011

Human resource (HR) information systems are employed extensively by modern day firms. They are designed to support the HR functions such as attracting job applicants (Stone, Lukaszewski, & Isenhour, 2005) automating training and development, managing employee performance, and administering benefits systems (Burkhard, Schooley, Dawson, & Horan, 2010; Strohmeier, 2007). HR information systems can help meet employee needs, streamline operating procedures, reduce operating expenses, and also increase information accuracy and accessibility. They also aid in improving the professional standing of HR professionals in the organization (Hussain,

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

Wallace, & Cornelius, 2007). Although they can offer a variety of benefits, they can also present problems. Prior researchers of HR information systems have studied factors such as design, implementation, system effectiveness (Stone, Stone-Romero, & Lukaszewski, 2003) and increased resistance to the system (Beckers & Bsat, 2002). However, there exists little research related to human resources security risk management (HRSRM). Since HR professionals deal with confidential data, security should be a top concern for HR professionals (Bussler & Davis, 2002).

Security risk management (SRM) is a series of mechanisms that an organization puts in place to counter or prevent an information security related event. Examples of such mechanisms include clearly defined information security policies, and implementation of secure computing practices (Blakley, McDermott, & Geer, 2001). HRSRM is a major subset of SRM that looks into how an organization's employee data must be protected from unauthorized access, disclosure, modification, destruction or interference (Calder, 2006). Information security on the other hand, at times referred to as computer security, is defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of information system resources (Stallings & Brown, 2008). At the center of this definition are three key objectives: confidentiality, integrity, and availability. Confidentiality assures that private information is not made available to unauthorized individuals. This is an important component to ensure privacy of employees' personal records (Wong & Thite, 2008). Integrity assures that information and programs are changed in a specified and authorized manner. Finally, availability assures that systems work promptly and service is not denied to users who are authorized.

The purpose of this study was to explore possible differences in perception between management and staff with regard to overall security risk management and human resource security risk management. We surveyed and interviewed management and staff at two Fortune 500 companies, heretofore referred to as Company A and Company B. The rest of the study is organized as follows. We highlight previous research in organizational information security and risk management, followed by presentation of our research questions and hypotheses. After that we present the research method, a discussion of results. Finally, we discuss limitations of the study and suggestions for future research before concluding.

Organizational Information Systems Security Research

Due to the inherent technical nature of the topic, information security has not been an area of active research in fields such as human resource management. However even in directly pertinent disciplines such as information systems, information security related research has not been extensive (Paulson, 2002; Zafar & Clark, 2009). The perceived intrusive nature of information security based studies has been mentioned as a leading cause of lack of research in this area (Kotulic & Clark, 2004).

Information security in previous literature has been equated with being of a technical, socio-philosophical (Ratnasingham, 1998), and/or a socio-organizational nature (Dhillon & Backhouse, 2001). Currently, some researchers argue that human factors should be considered since information systems are designed and implemented by people (Adams & Sasse, 1999; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). Examples of non-technical aspects of information security include culture, risk management, and regulatory compliance (Dhillon, 2007).

In a recent survey of over 400 senior IT professionals, 35% admitted using their administrative passwords to access confidential information such as human resource records, customer databases, marketing information, and layoff lists (Cyber-Ark, 2009). In addition, 18% of respondents reported incidents of information technology fraud or insider sabotage. However, organizational level studies that consider security of human resource management information systems in context of an actual business setting are currently lacking in HR information systems research.

Cultural theory postulates that the manner in which people interact socially is dependent upon their view of the world. The theory is based on four major world views: fatalism, hierarchy, egalitarianism, and individualism. Tsohou, Karyda, Kokolakis, and Kiountouzis (2006) applied cultural theory to information system risk management. They suggested strategies for IS risk management, depending on an individual's cultural bias. For example, fatalistic people perceive risk as unavoidable and tend to accept whatever guidelines or policies are imposed upon them. Conversely, individualists are less rule-bound and are more likely to accept guidelines or policies if they are accompanied by a cost-benefit analysis.

Since HRIS users interact with information systems on a regular basis in their business activities, how they use the systems and whether they follow established measures will ultimately influence the overall security of an organization's human resource information system. In essence, traditional IS security has a "behavioral root" (Workman & Gathegi, 2007) and is a subject of psychological and sociological actions of people (Parker, 1981). Most prior research in organizational IS security has dealt with success and failure of security policies. Protecting a system from the internal personnel involves deterrence, prevention, and containment of misuse (Theoharidou, et al., 2005). General deterrence theory (GDT) has been used to investigate the effect of organizational deterrent measures on computer abuses by employees. It suggests that deterrent measures can reduce computer abuse by potential offenders if the risk of punishment is high (deterrent certainty) and penalties for violations are severe (deterrent severity).

Effectiveness of Deterrence Measures

Findings regarding the effectiveness of deterrence measures have been mixed. In one study (Kankanhalli, Teo, Tan, & Wei, 2003), deterrent and preventive methods were found

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

to positively impact information security effectiveness. On the other hand, severity of the deterrence method did not have a significant impact. In a different study, Lee, Lee, and Yoo (2004) found that physical security systems (e.g. secured computer rooms) influenced a user's intention to install access control and intrusion detection software. In their study, two other factors: security policy and awareness did not have a significant impact. These results were not expected, according to GDT. In another study, an extended GDT model (D'Arcy, Hovav, & Galletta, 2009) was proposed to capture the antecedents of system misuse intention. They concluded that perceived severity of sanctions reduces the intention to misuse a system. The authors also found that security policy awareness does not increase user's perceptions of the likelihood of getting caught for any misuse. This is contrary to the GDT prediction of a positive relation between security policy awareness and the increased likelihood of getting caught. While the authors explained that this negative relation may be due to factors such as research design and user knowledge about the difficulties in detecting misuse incidents (D'Arcy, et al., 2009), it may be that user attitude toward the policies influenced the relation. A user may be under the impression that policies exist only on paper and will not be enforced, even though the punishments of violation may be severe. Therefore, employee actions will be reflected by that belief.

Social Bond Theory (SBT) is another most cited criminology that views the computer abuse as a result of the weakness or inexistence of social bonds. It assumes that despite a person's natural inclination to crimes, strong social bonds can deter crime (J. Lee & Lee, 2002; Theoharidou, et al., 2005). Lee, Lee, and Yoo (2004) proposed an integrative model based on GDT and SBT and investigated the IS insider computer abuse. The authors viewed social bonding as organizational trust that included attachment, commitment, involvement, and norms. Their study indicated that enhancement of social bonds through organizational trust such as participation in meetings and personal relationship with many people, could help reduce computer abuse by employees. Based on SBT, Theohardiou et al. (2005) suggest that an organization should focus on creating social bonds of attachment between staff and management, encourage employee participation in informal meetings to promote a team spirit, and also involve employees in all phases of security design and implementation to motivate them.

Some organizational information security studies have investigated employee security behaviors from an ethical perspective (Banerjee, Cronan, & Jones, 1998; Harrington, 1996; Leonard & Cronan, 2001). Ethics refers to informal norms and behaviors that may help deal with situations for which there are no formal rules or policies (Dhillon & Backhouse, 2000). A limitation in this line of research is that there is a general difficulty in classifying behaviors as being ethical or unethical. It is not always straightforward. According to prior studies (Calluzzo & Cante, 2004), some undesirable behaviors related to use of organizational IT property were viewed as being neither ethical nor unethical. An example of such behaviors is downloading files at the workplace or at an educational institution from the Internet for personal use.

Employee Security Policies Compliance

Prior organizational studies have also focused on employee compliance with security policies. In one such study, an Information Security Policy Compliance Model (Pahnila, Siponen, & Mahmood, 2007) suggests that a user's intention to comply with security policies is influenced by user attitude toward complying. The authors also state that attitude and intention are influenced by a mixture of negative and positive reinforcements. Examples of negative reinforcements include sanctions, threat appraisal, coping appraisal, and normative beliefs, whereas information quality of policies, facilitation conditions, and habits are examples of positive reinforcements. This model was tested via a survey of employees at a Finnish company. Results showed that sanctions did not have a significant impact on user intention to comply with information security policies. This result was contrary to the prediction of GDT. In another study, Workman, Bommer, and Straub (2008) contended that employee behavior depends on their assessment of the threat faced. This is based on the assumption that when a threat is perceived, employees will adjust their behavior according to the acceptable level of risk. An employee's perception of threat severity and vulnerability is a part of threat assessment.

Siponen and Vance (2009) proposed a neutralization model to study the problem of employee information security violations. Based on the neutralization theory in criminology literature, the model suggests that employees rationalize their violations of security policies. Neutralization techniques include: 1) defend by necessity, 2) appeal to higher loyalties, 3) condemn the condemners (justify by blaming the target of action), 4) justify bad behaviors with prior good behaviors, 5) justify by minimizing harm, and 6) deny responsibility. The study found that neutralization had significant effects on employee intention to violate information security policies. The effects of formal sanctions and information sanctions were not significant.

Exploring Organizational Information Security

The purpose of this study was to explore the perceptions of management and staff in regard to security risk management within the organization as a whole, as well as within the realm of human resource management. Our primary research questions and hypotheses include:

Research Question 1: Do management and staff differ in their perceptions of security risk management within an organization?

- H1: There is no significant difference between management and staff perceptions of organizational (or overall) security risk management

- H1a: There is no significant difference between management and staff perceptions of security risk management at Company A.

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

- H1b: There is no significant difference between management and staff perceptions of security risk management at Company B.

Research Question 2: Is perceived human resource security risk management a primary security concern to management and/or staff?

Research Question 3: Do perceptions of security risk management within an organization differ from those related to human resource security risk management?

- H2: There is no significant difference between perceptions of organizational security risk management and human resource security risk management.

- H2a: There is no significant difference between perceptions of security risk management and human resource security risk management at Company A.

- H2b: There is no significant difference between perceptions of security risk management and human resource security risk management at Company B.

Research Method

In this section we present how the sites and participants were selected, along with a description of the method used to ascertain construct validity and reliability of the study. This section concludes with an overview of the data collection process.

Site Selection and Participants

Management and staff at two Fortune 500 companies, heretofore referred to as Company A and Company B, were surveyed. Both companies are multinational technology firms with established security policies. We concentrated on a single location for each firm. Each location was within the United States, but in different parts of the country. In both companies, there were a greater number of staff participants, compared with management. However, this is not considered a limitation of the study, since an effective organization will typically have a pyramid structure (Sennewald, 2003). For the purpose of this paper, we are concentrating only on security risk management as it pertains to the organization as

a whole or human resources in general. A much larger survey was administered to the participants, but our focus is on the questions in Appendix A. Each of the questions is based on a 7 point Likert scale.

Construct Validity and Reliability

Seven professors and eleven doctoral students at a large North-Eastern university were asked to review the questionnaire. A security manager at Company A was asked to ascertain if the questions being asked were appropriate. This assisted in enhancing the construct validity of the questionnaire, as recommended by Nunnally and Bernstein (1994). Refinements were made with regard to the language, and the survey was then administered to 135 Company A employees to test for reliability and construct validity.

Two methods were used to gauge construct validity: confirmatory factor analysis (CFA) and the correlation between the constructs with the diagonal elements being the square root of the average variance extracted (AVE). In the case of CFA the factor loadings were above the suggested threshold of 0.6 (Chin, 1998). In addition to this, items that measured the same construct had higher loadings than those measuring other constructs. This suggests acceptable convergent and discriminant validity. With regard to the second approach, the AVE of each construct exceeded 0.5, which is considered the benchmark for convergent validity (Fornell & Larcker, 1981). Also, the square root of the AVE of each construct was greater than the correlation between the construct and other constructs, suggesting adequate discriminant validity.

Cronbach's alpha and composite reliability were used to assess reliability of the instrument. The alpha value and composite reliability for each construct was above 0.7, the suggested threshold for adequate reliability (Nunnally & Bernstein, 1994). The survey is attached in Appendix A.

Data Collection

Personnel at each of the two locations were asked to complete a web-based survey. Company A has 378 employees at the testing location, excluding those who participated in the validation and reliability portion of the study. Two-hundred and seventy-two responded to the survey, producing a response rate of 71.96%. One-hundred and fifteen out of 132 (87.12%) personnel at the Company B testing location responded to our survey. Overall response rate for both locations was 75.88%.

Discussion of Results

Tables 1 and 2 show the mean and standard deviation of the results from each of the survey questions. The higher mean value represents less favorable perception about security risk management. Note: questions twelve and thirteen apply specifically to human resource risk management. Since we have unequal sample sizes, the Independent Samples t-test was

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

used to test H1. Note that reverse coding was conducted on questions 8 and 9. Results are shown in Tables 4 and 5.

Table 1
Descriptive Statistics of the Results from Company A

Question	Management (n=87)		Staff (n=185)		Overall (n=272)	
	Mean	SD	Mean	SD	Mean	SD
1	2.04	0.89	2.01	1.05	2.03	0.99
2	2.29	1.44	4.23	1.46	3.61	1.71
3	2.37	1.39	4.37	1.38	3.73	1.67
4	2.39	1.47	4.28	1.52	3.68	1.75
5	2.51	1.33	4.55	1.34	3.90	1.64
6	2.89	1.55	4.27	1.44	3.83	1.61
7	2.44	1.25	4.18	1.44	3.62	1.61
8	2.40	1.24	4.32	1.62	3.72	1.75
9	2.49	1.30	4.42	1.56	3.80	1.73
10	2.09	1.05	2.07	0.94	2.08	0.98
11	2.43	1.34	4.30	1.47	3.70	1.68
12*	3.70	1.63	3.98	1.59	3.89	1.60
13*	3.17	1.70	4.46	1.41	4.05	1.63

* Questions pertaining specifically to HRSRM

Table 2
Descriptive Statistics of the Results from Company B

Question	Management (n=36)		Staff (n=79)		Overall (n=115)	
	Mean	SD	Mean	SD	Mean	SD
1	3.42	1.75	3.56	1.69	3.51	1.70
2	3.69	1.58	3.44	1.72	3.52	1.68
3	3.75	1.79	3.57	1.72	3.63	1.74
4	4.03	1.58	3.61	1.71	3.74	1.67
5	3.83	1.87	3.56	1.68	3.64	1.74
6	4.08	1.40	3.92	1.72	3.97	1.62
7	3.50	1.67	3.14	1.76	3.25	1.73
8	3.78	1.69	3.59	1.56	3.65	1.60
9	4.11	1.94	3.56	1.74	3.73	1.81
10	4.08	1.40	3.96	1.71	4.00	1.61
11	4.08	1.68	3.75	1.80	3.85	1.76
12*	3.56	1.61	3.81	1.77	3.73	1.72
13*	4.19	1.63	3.44	1.70	3.68	1.71

* Questions pertaining specifically to HRSRM

As shown in Table 3 (H1a), there was a significant difference in SRM perceptions between management and staff at Company A for 10 out of the 13 questions. They are questions 2 thru 9, 11, and 13 as follows: (The complete list of questions is included in Appendix A).

2) Internal operations that rely on accurate and timely data information have not been negatively impacted by security measures.

3) We have protective security measures in place that are cost-effective and have reduced the level of risk to acceptable levels.

4) The organization has a formal program of roles and responsibilities that are known to everyone.

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

5) The current security awareness program effort was in reaction in large part to actual or suspected past instances of security breaches at this location.

6) When a formal security policy initiative is launched, visibility is given to the event through devices such as management presentations and question/answer forums.

7) Management communicates visibly and seriously regarding the need to protect the confidentiality of sensitive information.

8) Getting authorization to access data that would be useful in my function is time consuming and difficult.

9) Data that would be useful to my function is unavailable because we do not have the right authorization.

11) The organization takes adequate steps in updating the SRM policy.

13) Personnel responsible for executing the security risk management process have sufficient experience to deal with security related incidents.

For each of these questions, staff had a less favorable perception (higher mean values) than management for Company A. Therefore, we reject the H1a null hypothesis for 10 out of 13 questions. Also, note the mean values for questions 12 and 13, the two questions specifically geared toward HRSRM. Note that neither management nor staff answered these questions favorably.

The difference in management and staff perceptions for Company B (Table 4) was not as great. Note that for Company B, management perceptions of SRM were, in general, more negative than those of staff. However, the only significant difference was seen in question 13: Personnel responsible for executing the security risk management process have sufficient experience to deal with security related incidents. Therefore, for H1b, we fail to reject the null hypothesis for all but question 13.

Table 3

Independent Samples t-test for Company A - Management versus Staff (95% CI).

		t-test				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Q1	Equal variances assumed	0.45	270.00	0.65	0.06	0.13
	Equal variances not assumed	0.48	196.47	0.64	0.06	0.12
Q2	Equal variances assumed	-10.28	270.00	0.00	-1.94	0.19
	Equal variances not assumed	-10.33	170.49	0.00	-1.94	0.19
Q3	Equal variances assumed	-11.14	270.00	0.00	-2.00	0.18
	Equal variances not assumed	-11.10	167.06	0.00	-2.00	0.18
Q4	Equal variances assumed	-9.64	270.00	0.00	-1.89	0.20
	Equal variances not assumed	-9.76	173.75	0.00	-1.89	0.19
Q5	Equal variances assumed	-11.78	270.00	0.00	-2.05	0.17
	Equal variances not assumed	-11.78	168.21	0.00	-2.05	0.17
Q6	Equal variances assumed	-7.22	270.00	0.00	-1.39	0.19
	Equal variances not assumed	-7.03	157.56	0.00	-1.39	0.20
Q7	Equal variances assumed	-9.67	270.00	0.00	-1.74	0.18
	Equal variances not assumed	-10.17	191.60	0.00	-1.74	0.17
Q8	Equal variances assumed	-9.63	270.00	0.00	-1.89	0.20
	Equal variances not assumed	-10.60	215.30	0.00	-1.89	0.18
Q9	Equal variances assumed	-10.00	270.00	0.00	-1.92	0.19
	Equal variances not assumed	-10.65	198.39	0.00	-1.92	0.18
Q10	Equal variances assumed	0.17	270.00	0.86	0.02	0.13
	Equal variances not assumed	0.16	153.18	0.87	0.02	0.13
Q11	Equal variances assumed	-10.10	270.00	0.00	-1.88	0.19
	Equal variances not assumed	-10.46	184.38	0.00	-1.88	0.18
Q12	Equal variances assumed	-1.33	270.00	0.18	-0.28	0.21
	Equal variances not assumed	-1.32	164.65	0.19	-0.28	0.21
Q13	Equal variances assumed	-6.54	270.00	0.00	-1.29	0.20
	Equal variances not assumed	-6.12	143.52	0.00	-1.29	0.21

DOI: 10.7885/1946-651X.1060

Table 4
Independent Samples t-test for Company B - Management and Staff Overall (95% CI).

		t-test				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Q1	Equal variances assumed	-0.41	113.00	0.68	-0.14	0.34
	Equal variances not assumed	-0.40	65.69	0.69	-0.14	0.35
Q2	Equal variances assumed	0.74	113.00	0.46	0.25	0.34
	Equal variances not assumed	0.77	73.41	0.44	0.25	0.33
Q3	Equal variances assumed	0.51	113.00	0.61	0.18	0.35
	Equal variances not assumed	0.51	65.37	0.61	0.18	0.36
Q4	Equal variances assumed	1.25	113.00	0.21	0.42	0.34
	Equal variances not assumed	1.29	72.97	0.20	0.42	0.33
Q5	Equal variances assumed	0.79	113.00	0.43	0.28	0.35
	Equal variances not assumed	0.76	61.53	0.45	0.28	0.37
Q6	Equal variances assumed	0.49	113.00	0.63	0.16	0.33
	Equal variances not assumed	0.53	81.96	0.60	0.16	0.30
Q7	Equal variances assumed	1.04	113.00	0.30	0.36	0.35
	Equal variances not assumed	1.06	71.40	0.29	0.36	0.34
Q8	Equal variances assumed	0.57	113.00	0.57	0.18	0.32
	Equal variances not assumed	0.55	63.00	0.58	0.18	0.33
Q9	Equal variances assumed	1.53	113.00	0.13	0.55	0.36
	Equal variances not assumed	1.47	61.61	0.15	0.55	0.38
Q10	Equal variances assumed	0.37	113.00	0.71	0.12	0.33
	Equal variances not assumed	0.40	81.52	0.69	0.12	0.30
Q11	Equal variances assumed	0.95	113.00	0.34	0.34	0.35
	Equal variances not assumed	0.97	72.36	0.33	0.34	0.35
Q12	Equal variances assumed	-0.74	113.00	0.46	-0.25	0.35
	Equal variances not assumed	-0.76	73.99	0.45	-0.25	0.33
Q13	Equal variances assumed	2.22	113.00	0.03	0.75	0.34
	Equal variances not assumed	2.26	70.31	0.03	0.75	0.33

In regard to the second research question, HRSRM does appear to be a primary security concern to both management and staff. For Company A, the management responses suggested negative perceptions toward HRSRM based on the results from questions 12 and 13 (highest mean values). And, staff were even more negative toward these questions than were management. For Company B, management expressed the greatest concern for question 13 (means of 4.19). Their mean response for this question was higher than that of staff (mean of 3.44). The combined results for both Companies A and B, as shown in

Table 5, indicate that two of the three highest mean values for management were associated with questions 12 and 13.

Table 5
Companies A and B

Question	Company A (n=272)		Company B (n=115)		Overall (n=387)	
	Mean	SD	Mean	SD	Mean	SD
1	2.03	0.99	3.51	1.70	2.47	1.42
2	3.61	1.71	3.52	1.68	3.58	1.70
3	3.73	1.67	3.63	1.74	3.70	1.69
4	3.68	1.75	3.74	1.67	3.70	1.72
5	3.90	1.64	3.64	1.74	3.82	1.67
6	3.83	1.61	3.97	1.62	3.87	1.61
7	3.62	1.61	3.25	1.73	3.51	1.65
8	3.72	1.75	3.65	1.60	3.70	1.70
9	3.80	1.73	3.73	1.81	3.78	1.75
10	2.08	0.98	4.00	1.61	2.65	1.49
11	3.70	1.68	3.85	1.76	3.75	1.70
12	3.89	1.60	3.73	1.72	3.84	1.64
13	4.05	1.63	3.68	1.71	3.94	1.66

Tables 6 and 7 show the comparison of means for overall SRM and HRSRM, broken down by management, staff, and organization (combined management and staff). To test for H2 (difference between SRM and HRSRM perceptions) we compared the organizational mean responses of overall SRM with the mean responses of HRSRM. Since sample sizes were equal, Paired Sample t-tests were conducted. As shown in Tables 8 and 9, we reject H2a, but fail to reject H2b. There was a significant difference in HRSRM perceptions versus SRM perceptions for Company A. The concern for HRSRM was greater than that of overall SRM. Although HRSRM appears to be a concern for both companies, there was no significant difference in HRSRM versus overall SRM perceptions for Company B.

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

Table 6
Company A - Responses for Overall SRM and HRSRM Related Questions

Question	Company A Management (n=87)		Company A Staff (n=185)		Organization (n=272)	
	Mean	SD	Mean	SD	Mean	SD
Overall SRM	2.40	0.92	3.91	1.06	3.43	1.23
HRSRM	3.44	1.43	4.22	1.24	3.97	1.35

Table 7
Company B- Responses for Overall SRM and HRSRM Related Questions

Question	Company B Management (n=36)		Company B Staff (n=79)		Organization (n=115)	
	Mean	SD	Mean	SD	Mean	SD
Overall SRM	3.85	1.40	3.61	1.39	3.68	1.39
HRSRM	3.88	1.18	3.63	1.21	3.70	1.20

Table 8
Paired Sample t-test Results of Company A – Overall SRM versus HRSRM

Paired Differences	Mean		-0.54
	Std. Deviation		1.50
	Std. Error Mean		0.09
	95% Confidence Interval of the Difference	Lower	-0.72
		Upper	-0.36
T			-5.98
Df			271
Sig. (2-tailed) at 95% CI			**0.00**

Table 9
Paired Sample t-test Results of Company B – Overall SRM versus HRSRM

Paired Differences	Mean		-0.02
	Std. Deviation		1.10
	Std. Error Mean		0.10
	95% Confidence Interval of the Difference	Lower	-0.23
		Upper	0.18
T			-0.22
Df			114.00
Sig. (2-tailed) at 95% CI			**0.83**

In summary, we found significant differences between management and staff perceptions regarding security risk management. This difference was most profound in Company A (10 out of 13 questions were significant). Based on overall mean values of the HRSRM questions (12 and 13), human resources security risk management appears to be a primary security concern. And, when further studied, there was a statistically significant difference in SRM versus HRSRM perceptions for Company A. HRSRM concerns were greater than overall SRM concerns. There was no significant difference between SRM and HRSRM perceptions for Company B although mean values of the HRSRM questions are higher than those of overall SRM questions.

Following administration of the survey, management and staff were requested to participate in a one-on-one interview to further discuss select issues. Following are some of the discussions related to HRSRM.

Employee Risk and Security Training

Employees interviewed were interested in knowing the background knowledge and experience of personnel who deal with security related issues. They were primarily concerned about employee privacy and confidentiality. They felt that in order to reduce human error, fraud, or misuse of the organization's HR information systems, those in charge of the process must be carefully screened, and mandated to go through education and training. According to Dhillon (2007), this can be done through focus on various security certifications such as Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA). According to the Gartner Group, security training and awareness provide the greatest return on investment (ROI) in information security (Schultz, 2004). However, since it is difficult to determine the direct benefits, employee training is generally the lowest priority on the list of information

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

security spending and is often the first area cut during budget reductions (Keller, Powell, Horstmann, Predmore, & Crawford, 2005).

Standardized Best Practice Guidelines

It has been highly recommended that firms publish and advocate information security guidelines for all systems (Stamp, 2006). Example guidelines include changing passwords frequently and not sharing employee identification numbers or passwords with anyone. An employee at Company A mentioned that a major portion of HRSRM guidelines are routinely "sent to each person with the understanding that procedures are kept fresh, and everyone is aware of any changes and updates." In regard to passwords, an employee in Company B stated that his password "is memorable to him, but not easily guessable by someone else." In both firms, employees are severely reprimanded if anyone leaves their desk while potentially sensitive files are open. In the case of Company A, there was at least one instance in which an employee was terminated because of the infraction. According to an executive, this was equivalent to "knowingly releasing confidential information from official records."

Exercise Physical Security

Employees at both Company A and Company B agreed, in principle, that security is not an issue that can be handled exclusively through software measures. For example, measures need to be taken to physically protect facilities, resources, and information from threat both internal and external to the company. Physical entry controls, security of data centers and computer rooms, equipment maintenance, and security disposal of equipment are some examples of the physical security systems (Lee et al., 2004).

A Company B employee highlighted a policy in which terminated employees are only allowed to go to their office to pick up personal belongings, and they must be accompanied by a guard. In many instances, employee accounts are either canceled or made inaccessible prior to the termination notification.

At Company A, physical security is present from the moment a person enters the front door. Visitors are not allowed to enter the premises without an escort. They must first pass through a scanner. Next, they are physically searched by a guard. Company A's employees only have to pass through the scanner, but may be randomly asked to volunteer for a physical search. Also, all lobbies, corridors, and common areas, such as the cafeteria, have closed circuit television monitoring.

Controlling Consultants and Contractors

Due to the nature of their business, both Companies A and B heavily interact with consultants and contractors. In regard to HR information systems, both firms have extensive contracts with Oracle in the shape of human resource management systems (HRMS) and customer relationship management (CRM) software. According to an executive at Company A, HR information systems security does not necessarily deal solely with control over its own employees. Since they delegate work to consultants and

contractors from outside firms such as Oracle, they are also delegating security. This point was shared by another Company A employee who expressed concern over contractors entering the premises, but without the same background checks required of employees.

Limitations and Future Research

This was an exploratory study that focused on two Fortune 500 technology companies that already had multiple security policies and guidelines in place. The results may not be generalizable to small and/or medium sized firms or those firms without established security policies and guidelines. Also, participation in both the survey and discussion were optional. Although we received high survey response rates from both companies, we had limited response in regard to the interviews.

This exploratory study adds to the existing literature by addressing security as it pertains to human resources. Future researchers should study a variety of firms, with focus on areas such as employee confidence in their HR information system, policies and guidelines specific to HR information systems, viability of physical controls, and guidelines for information security control when consultants and contractors have access to confidential data. Based on our experience, we recommend to researchers that the research method should be chosen carefully. Information security due to its intrusive nature may make participants hesitant with regard to sharing information of a sensitive nature. Quantitative results, along with interviews, can allay some of the concerns participants may have, in addition to providing greater context. We benefited from that.

Conclusion

In this study we explored possible differences in perception between management and staff with regard to overall security risk management and human resource security risk management policies and procedures at two Fortune 500 companies (Company A and Company B). We found significant differences in perceptions in Company A, whereas, the differences were not statistically significant in Company B. Our results provide strong support for the need for effective collaboration between HR, IT, and executive management. It also shows that additional security training and awareness are needed for HR professionals in order to have successful HRSRM. To our knowledge, this is one of the first studies that explores information security in the context of security risk management and human resource security risk management. As organizations continue to evolve with respect to human resource information systems, additional issues with regard to information security will need to be addressed.

DOI: 10.7885/1946-651X.1060

APPENDIX A

1) Relative to our type of industry, security is very effective at this location.

To a large extent						not at all
1	2	3	4	5	6	7

2) Internal operations that rely on accurate and timely data information have not been negatively impacted by security measures.

To a large extent						not at all
1	2	3	4	5	6	7

3) We have protective security measures in place that are cost-effective and have reduced the level of risk to acceptable levels.

To a large extent						not at all
1	2	3	4	5	6	7

4) The organization has a formal program of roles and responsibilities that are known to everyone.

To a large extent						not at all
1	2	3	4	5	6	7

5) The current security awareness program effort was in reaction in large part to actual or suspected past instances of security breaches at this location.

To a large extent						not at all
1	2	3	4	5	6	7

6) When a formal security policy initiative is launched, visibility is given to the event through devices such as management presentations and question/answer forums.

To a large extent						not at all
1	2	3	4	5	6	7

7) Management communicates visibly and seriously regarding the need to protect the confidentiality of sensitive information.

To a large extent						not at all
1	2	3	4	5	6	7

8) Getting authorization to access data that would be useful in my function is time consuming and difficult.

To a large extent						not at all
1	2	3	4	5	6	7

9) Data that would be useful to my function is unavailable because we do not have the right authorization.

To a large extent						not at all
1	2	3	4	5	6	7

10) The organization's business objectives and goals include compliance with a broad-level security policy.

To a large extent						not at all
1	2	3	4	5	6	7

11) The organization takes adequate steps in updating the SRM policy.

To a large extent						not at all
1	2	3	4	5	6	7

12) The organization offers sufficient security training to members who are directly involved with the security risk management process.

To a large extent						not at all
1	2	3	4	5	6	7

13) Personnel responsible for executing the security risk management process have sufficient experience to deal with security related incidents.

To a large extent						not at all
1	2	3	4	5	6	7

https://digitalcommons.kennesaw.edu/jekem/vol3/iss1/28
DOI: 10.7885/1946-651X.1060

References

Adams, A., & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM, 42*, 40-46.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly, 22*, 31-60.

Beckers, A., & Bsat, M. (2002). A DSS classification model for research in human resource information systems. *Information Systems Management, 19*, 1-10.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Workshop on New Security Paradigms* (pp. 97-104). Cloudcrodt, New Mexico: ACM New York, NY, USA.

Burkhard, R., Schooley, B., Dawson, J., & Horan, T. (2010). Information Systems and Healthcare XXXVII: When Your Employer Provides Your Personal Health Record—Exploring Employee Perceptions of an Employer-Sponsored PHR System. *Communications of the Association for Information Systems, 27*, 323-338.

Bussler, L., & Davis, E. (2002). Information systems: The quiet revolution in human resource management. *Journal of Computer Information Systems, 42*, 17-20.

Calder, A. (2006). *Information Security Based on ISO 27001/ISO 17799: A Management Guide* (1 ed.): Van Haren Publishing.

Calluzzo, V. J., & Cante, C. J. (2004). Ethics in information technology and software use. *Journal of Business Ethics, 51*, 301-312.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*, 7-16.

Cyber-Ark. (2009). *Trust Security & Passwords Survey Research Brief*. http://www.cyber-ark.com/pdf/Cyber-Ark_Spring_2009_Snooping_Survey.pdf. Accessed on: September 9, 2010

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*, 79-98.

Dhillon, G. (2007). *Principles of information systems security: text and cases*. Hoboken, NJ: Wiley.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*, 125-128.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*, 127-153.

Fornell, C., & Larcker, D. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research, 18*, 382-388.

Harrington, S. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*, 257-278.

Hussain, Z., Wallace, J., & Cornelius, N. (2007). The use and impact of human resource information systems on human resource management professionals. *Information & Management, 44*, 74-89.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*, 139-154.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management, 22*, 7-19.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*, 597-607.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management and Computer Security, 10*, 57-63.

Lee, S. M., Lee , S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*, 707-718.

Leonard, L. N. K., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: a study to explain influences. *Journal of the Association for Information Systems, 1*, 12.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3 ed.). NY: McGraw Hill.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior Towards IS Security Policy Compliance. In *40th Hawaii International Conference on System Sciences* (pp. 156b).

Parker, D. (1981). *Computer Security Management*. Reston, VA: Reston Publishing Company.

Paulson, L. (2002). Wanted: More network-security graduates and research. *Computer, 35*, 22-24.

Ratnasingham, P. (1998). Trust in Web-based electronic commerce security. *Information Management and Computer Security, 6*, 162-166.

Schultz, E. (2004). Security training and awareness-fitting a square peg in a round hole. *Computers & Security, 23*, 1-2.

Sennewald, C. A. (2003). *Effective security management* (4 ed.): Butterworth-Heinemann.

DOI: 10.7885/1946-651X.1060

Siponen , M., & Vance, A. (2009). Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, forthcoming.

Stallings, W., & Brown, L. (2008). *Computer Security: Principles and Practice*. Upper Saddle River, NJ: Pearson Prentice Hall.

Stamp, M. (2006). *Information security: principles and practice* (1 ed.). Hoboken, NJ.: Wiley-Blackwell.

Stone, D., Lukaszewski, K., & Isenhour, L. (2005). E-Recruiting: Online strategies for attracting talent. In H. G. Gueutal & D. Stone (Eds.), *The Brave New World of eHR: Human Resources Management in the Digital Age* (pp. 22-53). San Francisco, CA: Jossey-Bass.

Stone, D., Stone-Romero, E., & Lukaszewski, K. (2003). The functional and dysfunctional consequences of human resource information technology for organizations and their employees. In D. Stone (Ed.), *The functional and dysfunctional consequences of human resource information technology for organizations and their employees* (pp. 37-68). Greenwich, CT: JAI Press.

Strohmeier, S. (2007). Research in e-HRM: Review and implications. *Human Resource Management Review*, *17*, 19-37.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*, 472-484.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management and Computer Security*, *14*, 198-217.

Wong, Y., & Thite, M. (2008). Information Security and Privacy in HRIS. In M. Thite & M. Kavanagh (Eds.), *Human Resource Information Systems. Basics, Applications, and Future Directions* (pp. 395-407). Thousand Oaks, CA.: Sage Publications.

Workman, M., Bommer , W. H., & Straub, D. W. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*, 2799-2816.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, *58*, 212-222.

Zafar, H., & Clark, J. G. (2009). Current State of Information Security Research in IS. *Communications of the Association for Information Systems, 24*, 557-596.